Background of S/MIME

- Problems of existing secure e-mail systems
  - PEM : hard to implement
  - PGP : low security, hard to be compatible with existing e-mailing system

- Growth of S/MIME
  - IETF adopted S/MIME V2 as standard
  - many applications like Outlook(Microsoft), Communicator (Netscape), Eudora(Qualcomm) etc.
  - Many toolkits like S/MIME toolkit (RSA), S/MIME Freeware Library(VDA : J.A. Van Dyke and Association) etc.
RFC822

- "Standard for the format of ARPA Internet text message"
- Format for text message via e-mail
- Message = envelop + contents
  - env. : whatever information is needed to accomplish transmission and delivery
  - con. : compose the object to recipient
  - (ex) header line + unrestricted text (body) separate by blank line
  - header’s keyword : From, To, Subject, date, message ID etc
Limitation of SMTP/RFC822

- can’t send binary files
- can’t send 8 bit codes
- reject mail message over a certain size
- SMTP gateways translating ASCII to EBCDIC don’t use consistent set of mapping
- non-compatibility with X.400
- Some implementation problems
  - deletion, addition or reordering of CR and LF
  - Truncating or wrapping lines longer than 76 character
MIME (I)

- “Multipurpose Internet Mail Extensions”
  - rfc2045 MIME part 1 : Format of Internet message bodies
  - rfc2046 MIME part 2 : Media types
  - rfc2047 MIME part 3 : Message header extensions for Non-ASCII text
  - rfc2048 MIME part 4 : Registration procedure
  - rfc2049 MIME part 5 : Conformance criteria and examples
MIME(II)

- 5 Headers: MIME-version, Content-type, Content-transfer-Encoding, Content-ID, Content-Description
- Can express Multimedia e-mail
- Define Transfer encoding
- Compatible with rfc822
# MIME Content Type

<table>
<thead>
<tr>
<th>Type</th>
<th>Subtype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text</td>
<td>Plain</td>
<td>Unformatted text; maybe ASCII or ISO8859</td>
</tr>
<tr>
<td>Multipart</td>
<td>Enriched</td>
<td>Provides greater format flexibility</td>
</tr>
<tr>
<td>Multipart</td>
<td>Mixed</td>
<td>Different part independent,</td>
</tr>
<tr>
<td>Multipart</td>
<td>Parallel</td>
<td>No order defined same as Mixed</td>
</tr>
<tr>
<td>Multipart</td>
<td>Alternative</td>
<td></td>
</tr>
<tr>
<td>Multipart</td>
<td>Digest</td>
<td></td>
</tr>
<tr>
<td>Message</td>
<td>rfc822</td>
<td></td>
</tr>
<tr>
<td>Message</td>
<td>Partial</td>
<td></td>
</tr>
<tr>
<td>Message</td>
<td>External-body</td>
<td></td>
</tr>
<tr>
<td>Image</td>
<td>jpeg</td>
<td></td>
</tr>
<tr>
<td>Image</td>
<td>gif</td>
<td></td>
</tr>
<tr>
<td>Video</td>
<td>mpeg</td>
<td></td>
</tr>
<tr>
<td>Audio</td>
<td>Basic</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>PostScript</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>octet-stream</td>
<td></td>
</tr>
</tbody>
</table>
MIME transfer encoding

- 7 bit: short lines of ASCII char.
- 8 bit: short lines with non-ASCII char.
- Binary: non-ASCII + SMTP transportability
- quoted-printable
- base64: radix 64 encoding
- x-token: named nonstandard encoding
Features of S/MIME

- **Classification**
  - S/MIME : RSADSI
  - S/MIME v2 : RSADSI + multi-vendor consortium
  - S/MIME v3 : IETF + product vendor

- **Adding encryption function of MIME-style message**

- **Use PKCS #7 Cryptographic Message Syntax**

- **Use X.509 v3.**
Documents of S/MIME

- **V2**
  - S/MIME v.2 Message Specification (RFC2311)
  - S/MIME v.2 Certificate handling (RFC2312)

- **V3**
  - Cryptographic Message Syntax (draft-ietf-smime-cms)
  - S/MIME v.3 Message Specification (draft-ietf-smime-msg)
  - S/MIME v.3 Certificate Handling (draft-ietf-smime-cert)
  - Enhanced Security Service for S/MIME (draft-ietf-smime-ess)
S/MIME Goals

- Strong encryption
- Digital signatures
- Ease of use
- Flexibility trust to fit business
- Interoperability
- Exportability
S/MIME functionality

- Enveloped data: encrypted content of any type and encrypted-content encryption key for one or more recipients
- Signed data: digital signature + encrypting with private key + base64 encoding
- Clear-signed data: signed data + base64 encoded digital signature
- Signed and enveloped data: signed-only and encrypted-only nested, so that encrypted data may be signed and signed data or clear-signed data may be encrypted
Message of S/MIME

- Clear data
- Signed data
- Enveloped data
- Signed and enveloped data
Scalable Trust

- Direct Trust
- Cross certification
- (Hierarchical) Certification Authority
S/MIME Certificate Handling

- X.509 CA + PGP’s Web of trust
- S/MIME managers and users must configure each client with a list of trusted keys and with CRL
- local responsibility for maintaining certificates to verify incoming signature and to encrypt outgoing message
- UA’s role: Key generation, Registration, Certificate storage and retrieval
CA service

- Verisign
- GTE
- U.S. Postal Service
- KISA
- KT/ Dacom
- 3 big parties (EC, banking, security) etc
Key storage of S/MIME

- Use certificate

X.509 Certificate Format Ver.3.0

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Serial Number</th>
<th>Algorithm ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature Info</td>
<td>Issuer</td>
<td>Parameters</td>
</tr>
<tr>
<td>Validity period</td>
<td>Subject</td>
<td></td>
</tr>
<tr>
<td>Subject</td>
<td>Public Key Info</td>
<td>Algorithm ID</td>
</tr>
<tr>
<td>Certificate Signature</td>
<td>Subject Public Key</td>
<td></td>
</tr>
</tbody>
</table>
Features of S/MIME v3

- Use DSA, DH-PKC
- Use SHA-1
- Signed receipts: signing by receiver’s private key of signed message for proof of delivery
- Security labels: access right to original message
- Secure mailing lists: In case of multiple receivers, MLA (Mail List Agent) sends encrypted message per a receiver.
S/MIME Support

AOL
Banyan
Blue Mountain
CommerceNet EDI Pilot
*ConnectSoft
*Deming
*Frontier Technologies
FTP
GlobalKey
Harbinger
Lotus
Microsoft(**)
Netscape
Nortel
Novell
*OpenSoft
Premenos
Qualcomm(**)
SecureWare
Sterling
*Verisign

* : Direct Support
** : Plug-in
S/MIME is a specification for secure electronic messaging. In 1995, several software vendors got together and created S/MIME to solve a very real problem - interception and forgery of e-mail. Protecting sensitive data is a real concern, especially in a world that is becoming increasingly more wired. The goal of S/MIME is to make it easy to secure messages from prying eyes. Since its creation, S/MIME has come a long way.

S/MIME is short for Secure MIME. The specification was designed to be easily integrated into e-mail and messaging products. S/MIME builds security on top of the industry standard MIME protocol according to an equally important set of cryptographic standards, the Public Key Cryptography Standards (PKCS). The fact that S/MIME was created using other standards is important for something that is likely to be widely implemented.

(c)ICU Kwangjo Kim
## Comparison of PGP and S/MIME(I)

<table>
<thead>
<tr>
<th>Packaging Signing</th>
<th>PGP 2.6</th>
<th>PGP/ MIME</th>
<th>PGP 5.0</th>
<th>OpenPGP</th>
<th>S/MIME v2</th>
<th>S/MIME v3</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Classic)</td>
<td>(IETF)</td>
<td>(IETF)</td>
<td>(IETF)</td>
<td>(IETF)</td>
<td>(IETF)</td>
<td>(IETF)</td>
</tr>
<tr>
<td>Special (Text in Body)</td>
<td>MIME</td>
<td>Special, MIME</td>
<td>MIME</td>
<td>MIME, Special</td>
<td>MIME, CMS</td>
<td>MIME</td>
</tr>
<tr>
<td>Encrypting</td>
<td>Special</td>
<td></td>
<td></td>
<td>PKCS#7</td>
<td>CMS</td>
<td></td>
</tr>
<tr>
<td>Records</td>
<td>Special Binary</td>
<td></td>
<td></td>
<td>PKCS#7</td>
<td>CMS</td>
<td></td>
</tr>
<tr>
<td>Transport Protection</td>
<td>Special (ASCII Armor)</td>
<td>MIME and Special</td>
<td>Special</td>
<td>MIME, Special</td>
<td>MIME</td>
<td></td>
</tr>
<tr>
<td>Selection</td>
<td>Special Binary</td>
<td></td>
<td></td>
<td>PKCS#7</td>
<td>CMS</td>
<td></td>
</tr>
<tr>
<td>Algorithms Certificate</td>
<td></td>
<td>Special (Web of trust)</td>
<td></td>
<td>X.50 (PK)</td>
<td></td>
<td>9 v3 Diffie-Hellman (X9.42), RSA</td>
</tr>
<tr>
<td>Session</td>
<td>RSA</td>
<td>ElGamal, RSA</td>
<td>ElGamal</td>
<td>RSA</td>
<td></td>
<td>Diffie-Hellman (X9.42), RSA</td>
</tr>
<tr>
<td>Digest</td>
<td>MD5</td>
<td>SHA-1, MD5</td>
<td>5</td>
<td>SHA-1, MD5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signed</td>
<td>RSA</td>
<td>DSA, RSA</td>
<td>RSA</td>
<td>RSA</td>
<td></td>
<td>DSA, RSA</td>
</tr>
<tr>
<td>Encrypt</td>
<td>IDEA</td>
<td>CAST5, IDEA, TripleDES</td>
<td>TripleDES (EDE), IDEA, CAST5</td>
<td>RC2-40, TripleDES</td>
<td></td>
<td>TripleDES (CBC), RC2-40, DES</td>
</tr>
</tbody>
</table>
Description

- Signing, Encrypting: Packaging sections of data and control information into Internet Mail and distinguishing between the sections
- Records: Separating internal information "records" and fields
- Transport Protection: Protection data against vagaries of transport services -- especially email transport -- by adding a layer of data encoding, for example, so that trailing white spaces are not eliminated.
- Selection: Mechanism for specifying choices among algorithms etc.
- Certificate: Associating identifiers with keys and validating the association
- Session: Public key mechanism for exchanging random session keys between correspondents
- Digest: Algorithm(s) for performing data integrity hash calculation
- Signed: Algorithm(s) for encrypting content digest to achieve data authentication
- Encrypt: Algorithm(s) supported for encrypting content data to achieve privacy
# Comparison of PGP and S/MIME(II)

## Others

<table>
<thead>
<tr>
<th>Class</th>
<th>PGP</th>
<th>S/MIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication policy</td>
<td>Distributed authentication</td>
<td>Hierarchical authentication</td>
</tr>
<tr>
<td>Key storage</td>
<td>Key ring</td>
<td>Key certificate</td>
</tr>
<tr>
<td>Standard</td>
<td>-</td>
<td>IETF</td>
</tr>
<tr>
<td>Commercialization</td>
<td>No compatibility test</td>
<td>Compatibility test</td>
</tr>
<tr>
<td></td>
<td>Small products</td>
<td>Many commercial products</td>
</tr>
<tr>
<td>Main Usage</td>
<td>Personal</td>
<td>Company, Enterprise</td>
</tr>
</tbody>
</table>

(c)ICU Kwangjo Kim